

# (19) 대한민국특허청(KR) (12) 공개특허공보(A)

(51) Int. Cl. <sup>6</sup> H04K 01/04	(11) 공개번호 특 1995-0013093
	(43) 공개일자 1995년 05월 17일
(21) 출원번호 (22) 출원일자	특 1994-0026435 1994년 10월 15일
(30) 우선권 주장	93-260754 1993년 10월 19일 일본(JP) 93-279529 1993년 10월 19일 일본(JP)
(71) 출원인	마쯔시다덴기산교 가부시키가이샤 모리시타 요이찌 일본국 오오사카후 가도마시 오오아자가도마 1006반지
(72) 발명자	카타 노보루 일본국 효고켄 이타미시 카스가오카 1-44 무라카미 히로키 일본국 오오사카후 오오사카시 요도가와구 신타카 1-12-1-1011 이바라키 스스무 일본국 오오사카후 토요나카시 히가시토요나카쵸 3-23-A-302 나카무라 세이지 일본국 오오사카후 토요나카시 무코우가오카 1-6-1-502
(74) 대리인	신중훈, 임옥순

심사청구 : 있음

## (54) 스크램블전송장치 및 난수발생장치

### 요약

본 발명은, 디지털부호화된 신호의 전송 혹은 보관에 있어서, 신호를 교반하고, 복호 순서를 허가된 것에만 부여함으로써, 재생할 수 있는 것을 한정하는 신호교반을 행하는 스크램블장치 및 그것을 재생하는 디스크램블장치에 관한 것이며, 특히, 재생할때까지 일어나는 착오에 대해서 높은 재생복귀능력을 가진 스크램블전송장치에 관한 것으로서, 원신호가 가변길이부호를 포함한 신호라도 비트착오가 발생했을때, 재생이 복귀할때까지의 기간이, 스크램블처리를 하지 않는 경우와 동등한 스크램블전송장치를 제공하고, 또, 스크램블을 행하기 위하여 하나의 난수발생장치에 의해 복수의 출력을 가지고, 그 각각으로부터 출력되는 난수열이 각각 독립적인 난수로하고 이용가능한 난수발생장치를 제공하는 것을 목적으로 한 것이며, 그 구성에 있어서, 스크램블장치는, 가변길이 부호를 포함한 디지털데이터를 스크램블키에 의거해서 스크램블처리하는 스크램블장치와 스크램블키에 의거해서 재생처리하는 디스크램블장치와 스크램블키 전송부로 이루어진다. 스크램블장치가 가변길이 부호는 포함한 디지털데이터를 소정의 교반키에 의해서 결정하는 규약에 의거해서 교반처리하는 교반처리부와 교반처리부에 교반키를 부여하는 교반키갱신부로 이루어진다. 교반키는 스크램블키에 의거 해서 생성한다. 교반키 갱신부가, 입력 데이터중에서 재생의 동기를 취할 수 있는 최소의 데이터단위 마다 새로운 교반키를 교반처리부에 부여한다. 디스크램블장치가, 가변길이부호를 포함한 디지털데이터중의 스크램블된 데이터를 교반키에 의해서 결정하는 규약에 의거해서 디스크램블처리하는 역변환처리부와 역변환처리부에 교반키를 부여하는 교반키갱신부로 이루어진다. 교반키갱신부가 전송되어오는 스크램블키를 근거로 교반키를 생성하는 교반키 생성부를 가지고, 생성된 교반키를 입력데이터중에서 재생의 동기를 취할 수 있는 최소의 데이터단위마다 새로운 교반키를 역변환처리부에 부여한다. 스크램블의 동기가 재생의 동기와 동일한 안정된 스크램블동기를 실현할 수 있다. 교반에 사용하는 난수발생기는, 간단한 구성으로 한번에 복수비트의 출력을 얻을 수 있는 것을 특징으로 한 것이다

### 대표도

### 도1

### 명세서

[발명의 명칭]

스크램블전송장치 및 난수발생장치

[도면의 간단한 설명]

제1도는 본 발명의 실시예에 있어서의 스크램블전송장치,

제3도는 실시예에 있어서의 난수발생장치 (2) 및 배타적논리합회로(4)의 상세도,

제4도는 본 발명의 제2실시예에 있어서의 난수발생장치의 구성도.

본 내용은 요부공개 건이므로 전문 내용을 수록하지 않았음

### (57) 청구의 범위

#### 청구항 1

가변길이부호를 포함한 디지털데이터를 스크램블키에 의거해서 스크램블처리하는 스크램블장치와 스크램블키에 의거해서 재생처리하는 디스크램블장치와 스크램블키 전송수단으로 이루어지고, 스크램블장치가 가변길이부호를 포함한 디지털데이터를 소정의 교반키에 의해서 결정하는 규약에 의거하여 교반처리하는 교반처리수단과 상기 교반처리수단에 상기 교반키를 부여하는 교반키갱신수단으로 이루어지고, 교반키는, 상기 스크램블키에 의거해서 생성하고, 상기 교반키갱신수단이, 입력데이터중에서 재생의 동기를 취할 수 있는 최소의 데이터 단위마다 새로운 교반키를 교반처리수단에 부여하는 스크램블장치이며, 디스크램블장치가, 가변길이부호를 포함한 디지털데이터중의 스크램블된 데이터를 교반키에 의해서 결정하는 규약에 의거하여 디스크램블처리하는 역변환처리수단과 상기 역변환처리수단에 상기 교반키를 부여하는 교반키갱신수단으로 이루어지고, 교반키갱신수단이 전송되어오는 스크램블키를 근거로 교반키를 생성하는 교반키생성수단을 가지고, 생성된 교반키를 입력데이터중에서 재생의 동기를 취할 수 있는 최소의 데이터단위마다 새로운 교반키를 역변환처리수단에 부여하는 디스크램블장치인 것을 특징으로 하는 스크램블전송장치.

#### 청구항 2

제1항에 있어서, 전송데이터가 MPEG표준에 준거한 데이터로서, 스크램블키갱신수단이, Group of picture의 사용자데이터영역에 스크램블키정보를 채워넣는 채워넣기수단을 가진 것을 특징으로 하는 스크램블전송장치.

#### 청구항 3

가변길이부호를 포함한 디지털데이터를 소정의 교반키에 의해서 결정하는 규약에 의거하여 교반처리하는 교반처리수단과 상기 교반수단에 상기 교반키를 부여하는 교반키갱신수단으로 이루어지고, 교반키는, 스크램블키에 의거해서 생성가능하고, 상기 교반키갱신수단이, 입력데이터중에서 재생의 동기를 취할 수 있는 최소의 데이터단위마다 새로운 교반키를 교반처리장치에 부여하는 것을 특징으로 하는 스크램블장치.

#### 청구항 4

제3항에 있어서, 입력데이터가 MPEG표준에 준거한 영상신호로서, 교반키갱신수단이, 입력데이터중의 슬라이스단위마다 새로운 교반키를 교반장치에 부여하는 것을 특징으로 하는 스크램블장치.

#### 청구항 5

제4항에 있어서, 교반장치는, 코드검출부와 난수발생기 및 배타적논리합회로로 이루어지고, 코드검출부는, 입력신호중의 스크램블의 대상이 되는 부호를 검출하여, 검출결과를 난수발생기에 보내고, 난수발생기는, 검출코드중의 스크램블의 대상비트수의 난수치를 생성하고, 배타적논리합회로, 난수발생출력과 입력신호의 배타적논리합연산을 행하는 것을 특징으로 하는 스크램블전송장치.

#### 청구항 6

가변길이부호를 포함한 디지털데이터중의 스크램블된 데이터를 교반키에 의해서 결정하는 규약에 의거하여 디스크램블처리하는 역변환처리수단과 상기 역변환처리수단에 상기 교반키를 부여하는 교반키갱신수단으로 이루어지고, 교반키갱신수단이 전송되어오는 스크램블키를 근거로 교반키를 생성하는 교반키생성수단을 가지고, 생성된 교반키를 입력데이터중에서 재생의 동기를 취할 수 있는 최소의 데이터단위마다 새로운 교반키를 역변환 처리수단에 부여하는 것을 특징으로 하는 디스크램블장치.

#### 청구항 7

제6항에 있어서, 교반키갱신수단이, 생성한 교반키를 입력데이터의 슬라이스단위마다 역변환처리장치에 부여하는 것을 특징으로 하는 디스크램블장치.

#### 청구항 8

제7항에 있어서, 역변환처리수단은, 코드검출부와 난수발생기 및 배타적논리합회로로 이루어지고, 코드검출부는, 스크램블된 부호를 검출하고, 검출결과를 난수발생기에 보내고, 난수발생기는, 검출코드중의 스크램블의 대상비트수의 난수치수를 생성하고, 배타적논리합회로, 난수발생출력과 입력신호의 배타적논리합연산을 행하는 것을 특징으로 하는 디스크램블장치.

#### 청구항 9

비트를 기억하는 복수의 기억수단과 각 기억수단이 기억하는 신호를 각각 인접하는 기억수단에 시프트시키는 동시에 기억수단에 기억된 비트치의 선형결합한 값을 피크백하는 시프트 및 피크백수단으로 이루어진 M계열 난수발생수단과 적어도 하나 이상의 배타적논리합연산수단을 구비하고, 각배타적논리합수단은, 상기 M계열난수발생수단중의 복수의 기억수단의 출력의 배타적논리합결합을 연산하는 배타적논리합수단이고, 상기 M계열난수발생수단중의 기억수단의 출력 혹은 배타적논리합수단의 출력으로 이루어진 복수의 난수출력을 가진 것을 특징으로 하는 난수발생장치.

청구항 10

제9항에 있어서, M계열난수발생수단중의 피드백수단이 그 피드백방법을 표시한 원시다항식이, 서로 상반다항식이 되는 2가지의 피드백수단을 가지고, 제어 신호에 의해서 2개의 피드백수단의 어느한쪽을 선택하는 선택수단을 구비한 피드백수단인 것을 특징으로 하는 난수발생장치.

청구항 11

난수발생수단과 복수비트를 기억하는 기억수단과 논리곱회로를 구비하고, 기억수단은, 난수발생수단의 출력동기해서 기억하고 있는 신호를 1순회시프트하고, 논리곱회로는, 난수발생장치의 각각의 출력과 기억수단의 비트출력과의 논리곱을 출력하는 것을 특징으로 하는 난수발생장치.

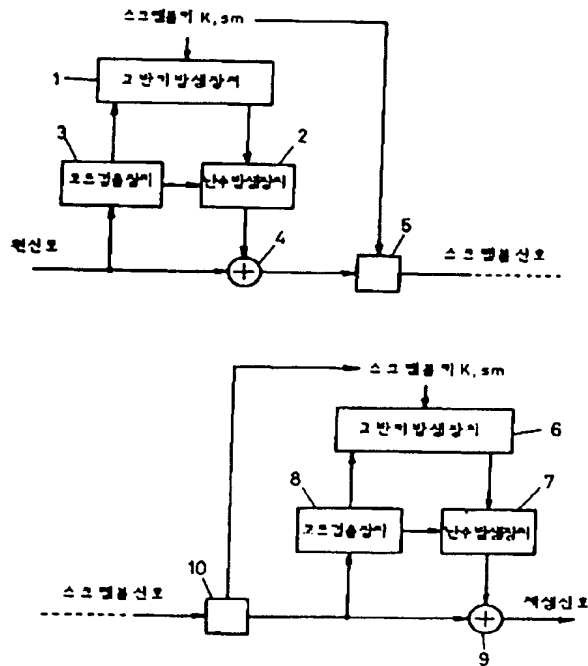
청구항 12

제3항에 있어서, 난수발생수단이, M계열난수발생수단중의 피드백수단이 그 피드백방법을 표시한 원시다항식이, 서로 상반다항식이 되는 2가지의 피드백수단을 가지고, 제어 신호에 의해서 2개의 피드백수단의 어느한쪽을 선택하는 선택수단을 구비한 피드백수단인 것을 특징으로 하는 난수발생장치.

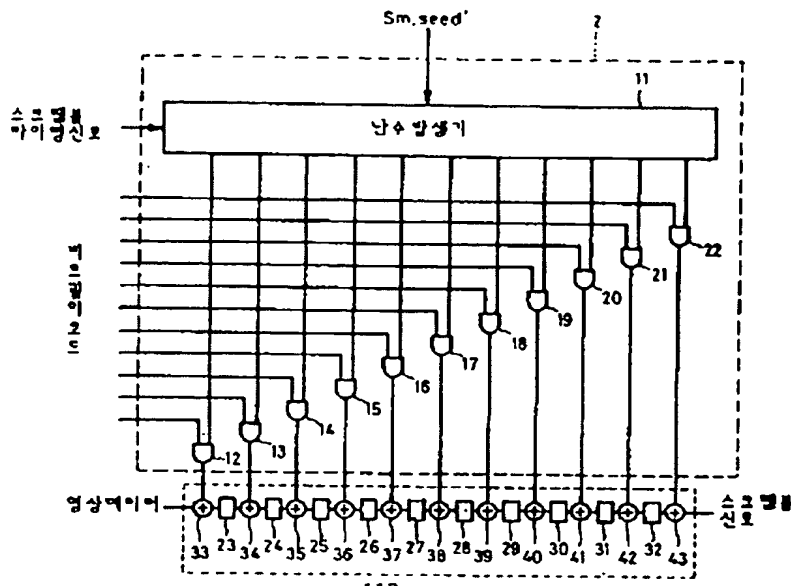
※ 참고사항 : 최초출원 내용에 의하여 공개하는 것임.

도면

도면1



도면3



도면4

